DIVISION OF
PUBLIC SAFETY & SECURITY
UNIVERSITY OF MICHIGAN

Standard: Retention and Release of Security Camera Recorded Images

Security camera and video surveillance recorded images may be accessed, used, or disclosed by authorized U-M systems users only when necessary for

- maintenance of public safety and security;
- investigation or prosecution of illegal activity;
- compliance with legal obligations to preserve, release, or otherwise use such images.

Specific terms and conditions for the accessing, retaining, and releasing of these images, including guidelines for the sharing of images internal to U-M departments, are defined in this**Retention and Release of Security Camera Recorded Images Standard**.

Several SPGs provide additional policy requirements for units with security camera installations and their authorized system operators. Specifically, those SPGs are:

1. SPG 601.12, **Institutional Data Resource Management Policy**
2. SPG 601.27, **Information Security Policy**
3. SPG 601.7, **Proper Use Of Information Resources, Information Technology, and Networks at the University of Michigan**
4. SPG 601.12, **Institutional Data Resource Management Policy**

Security camera system operators and supervisorsare responsible to appropriately protect the privacy of personal information that may have been captured by cameras under their control. They are subject to disciplinary action, as described in SPG 601.7 and SPG 201.12, for violations of these retention and release standards.

Specifically, images recorded by security camera systems are considered sensitive information whose confidentiality, integrity, and availability should be protected as provided for in SPG 601.27, **Information Security Policy**. Sensitive information refers to information whose unauthorized disclosure may have serious adverse effect on the university's reputation, resources, services, or individuals. Information with significant proprietary, ethical, or privacy considerations or protected under federal or state regulations is typically classified as sensitive.

Video surveillance records are further defined as institutional data in accordance with SPG 601.12, **Institutional Data Resource Management Policy**. Security camera recordings will be considered Business/Finance data that fall under the aegis of the Business/Finance data steward (**U-M Data Administration Guidelines for Institutional Data Resources**).

Secure Storage of Security Camera Recorded Images

All recorded images generated by U-M security cameras must be stored in a secure location established by the operating unit, accessible only to authorized and trained operators and supervisors, and configured to prevent unauthorized access, modification, duplication, or destruction.

Preservation and Retention of Security Camera Recorded Images

Recorded images should be retained for no more than 30 days.

Recordings must be erased or recorded over in a secure manner after 30 days in the absence of a compelling reason to retain or a request from the Executive Director, Division of Public Safety and Security, Office of the General Counsel or the Executive Vice President and Chief Financial Officer. Units should follow the procedures provided by Property Disposition (http://www.finance.umich.edu/analysis/property-disposition/departments/computers) to sanitize, wipe, or destroy devices with recorded images.

Exceptions that may permit or require retention longer than 30 days include:

- Ongoing criminal or civil court proceeding, employment investigation, or other legal hold or court order
- Demonstrated business need approved by the EVP/CFO or delegated authority
- Grantor or funding agency requirement

The EVP/CFO or delegated authority must approve in advance and in writing the preservation and storage by any unit of all other security camera data for greater than 30 days.

Release of Security Camera Recorded Images

Freedom of Information Act (FOIA) requests received by units for recorded images must be forwarded to the U-M FOIA Office. The FOIA office will make the determination as to whether the images will be provided or are exempt from release.

Subpoenas, search warrants, court orders and any other legally enforceable requests received by units for recorded images must be forwarded immediately after receipt to the Office of the General Counsel, which is responsible for reviewing and responding to all such requests.

Departments must provide access to or copies of stored video images upon request, unless prohibited by law, to the U-M Police Department (UMPD) as needed in connection with any ongoing criminal investigation. Any other internal-to-campus request for access to or release of recorded images must be forwarded to the EVP/CFO or delegated authority, which will review the request and make the final determination. No unit personnel, including the dean or director, can make such determination.

Security Camera Recorded Image Logs

All units that operate security cameras must maintain a logbook to record all activities related to the equipment and records. Activities include information regarding the use and maintenance and repair of equipment. This logbook must remain in a safe and secure location, available only to authorized operators or administrators.

Security camera systems operators must maintain a log of all instances of access to and release of security camera recorded material, including any breaches or unauthorized disclosures. The log entry should include:

1. Review of records by authorized security camera systems operators: time and date of review; reason for review; name of reviewer.
2. Request for access or release of records by internal U-M unit or external law enforcement or other agency: Originator of request for access or release of records, including agency, department, or individual, contact information, reason for request, and time and date request was received; approval or denial of request for access or release of records, including approver's name, and time and date response was sent to requestor; access or release of records information, including time and date, format of records accessed or released, viewer or recipient of records, and name of operator that provided the records.
3. Unauthorized disclosure or access to security camera records: time and date of breach if known, how breach was discovered, source of breach; unauthorized recipient or viewer of records if known.
4. Authorized Erasure or Destruction of Recorded Images: preserved materials must be destroyed in a secure manner as soon as they are no longer needed for the purpose for which they were preserved (assuming there is no legal further legal requirement to preserve them).
5. Loss of Backup or Saved Recorded Images: time and date of loss of recorded images due to technical problem or failure or inadvertent or accidental destruction

Unauthorized Loss, Access, Release, or Destruction

Any incident involving unauthorized loss, access to, or release or destruction of security camera recorded images must be reported to the Office of the EVP/CFO within 24 hours of the incident being identified or initially reported to the unit.